APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/667,834	09/22/2003	Jian Zhang	CN920020008US1	1003

7590   12/24/2008

Louis P. Herzberg
Intellectual Property Law Dept.
IBM Corporation
P.O. Box 218
Yorktown Heights, NY 10598

EXAMINER
PARRA, OMAR S

ART UNIT	PAPER NUMBER
2421	

MAIL DATE	DELIVERY MODE
12/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/667,834	ZHANG ET AL.
Office Action Summary	Examiner	Art Unit	
	OMAR PARRA	2421	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *08/01/2008*.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1,2,4-10,12-17 and 19-37* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1,2,4-10,12-17 and 19-37* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

08/01/2008 has been entered.

Response to Arguments

2.   Applicant's arguments with respect to claims 1, 2, 4-10, 12-17 and 19-37 have

been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims **1, 2, 9, 10, 10, 17 and 22-33** are rejected under 35 U.S.C. 103(a) as

being unpatentable over Simmons et al. (hereinafter 'Simmons', Corrected Pub. No.

2006/0085821, of record) in view of NPL document "Introduction to SSL" (hereinafter

'SSL' reference, of record) in further view of Lupulescu et al. (hereinafter 'Lupulescu',

Pub. No. 2003/0030751).

Regarding claims 1, 9, 17 and 22-33, Simmons teaches a Video-on-Demand system (with respective method and computer readable medium) for demanding a video program via a short message, comprising:

short message generating means for receiving a user demand **(User interface 54, Fig. 2; [0040] lines 1-8)**, and generating a demand short message based on the user demand, said demand short message including at least a User Identifier field, a Program Identifier field of the demanded video program and an Authentication field **([0017]; [0040] lines 1-15; [0044] lines 22-[0045]; [0052])**;

short message sending means for sending the demand short message generated by the short message generating means **(Network connectivity 12, Fig.2; ;**

demand short message processing means **(Transaction server 10, Fig. 1)** at a program delivering end for receiving the demand short message, processing the received demand short message to extract the user identifier and using the Authentication field to authenticate the legality of the user, and sending the program identifier of the demanded program by a legal user to video delivering means **([0040]; [0044]; [0045])**;

video delivering means **(Content Providers 6, Fig. 1)** for sending program content corresponding to the program identifier from the program delivering end to the user end indicated by a legal user identifier **([0040]- [0045])**; and

program playing means at the user end for receiving the video program sent by the video delivering means and playing it back to the user **(42, Fig. 2)**.

On the other hand, although Simmons teaches that secure socket layer (SSL) can be implemented; he does not teach the details of the implementation of the security and the encryption of the content.

However, in an analogous art, the article "Introduction to SSL" teaches that when communication between server and user is to be established, authentication certificates along with other information to first authenticate each other and share keys and once authentication is performed encryption and decryption of the content is performed with the shared keys (page 1 and 2, paragraphs 7 and 8; paragraph 21 numerals 1-10). Additionally, the 'SSL' teaches that a format or ciphers to be used are established between client and server for communicating between them (page 6, numerals 1-3). The article teaches that for giving more security while transmitting, all data transmitted is encrypted using different level of ciphers such as MD5, which creates a digest of the message (all fields transmitted) (pages 2 and 3, paragraphs 11 and 12; or table 1 listing all the ciphers that support key exchange).

Therefore, it would have been obvious to an ordinary skilled in the art at the time of the invention to modify Simmons's system to include SSL as a security measure as taught by NPL document, for authenticated and encrypted communication between clients and servers ("Introduction to SSL", paragraph 1).

Additionally, the combined teachings of Simmons and the 'SSL' reference teach all the limitations as explained above. On the other hand, Simmons and the 'SSL' reference do not explicitly teach the short message sending means comprising a mobile phone device for sending said demand short message via a wireless connection.

However, in an analogous art, Lupulescu teaches a system that uses a cell
phone or PDA to send a message requesting the purchase of a On-demand or PPV
event or movie through a wireless network (Title; abstract; [0011]; [0013]; [0015];
[0028]-[0031]).

Therefore, it would have been obvious to an ordinary skilled in the art at the time
of the invention to have modified Simmons and 'SSL's invention with Lupulescu's way of
sending a On-demand request message through a cell phone or PDA for the benefit of
not limiting the costumer to having to order a PPV event only through non-mobile 'PC or
permanent telephone connection to the subscriber's television receiver' (Lupulescu:
[0009]).

Regarding claims 2 and 10, the combined teachings of Simmons and the 'SSL'
reference teach a Video-on-Demand further comprising the step of sending from the
program delivering end to the user end a reply message including a confirmation
message indicating that the demand short message has been received **(Simmons: The
user knows that his request was received when he/she receives the files, [0044]
lines 32-37; or when the PIN is sent, which can be sent with the request [0052], a
message is sent if it is not verified, [0049]).**

5.   Claims **4- 8, 12-16 and 19-21** are rejected under 35 U.S.C. 103(a) as being
unpatentable over Simmons et al. (hereinafter 'Simmons', Corrected Pub. No.

2006/0085821, of record) in view of NPL document "Introduction to SSL" (hereinafter

'SSL' reference, of record) in view of Lupulescu et al. (hereinafter 'Lupulescu', Pub. No.

2003/0030751) in further view of Needham et al. (hereinafter 'Needham', Pub. No.

2003/0177495, of record).

Regarding claims 4, 12 and 19, the combined teachings of Simmons, the 'SSL'

reference and Lupulescu teach all the limitations of the claims they depend on.

Simmons and the 'SSL' reference also teach a video-on-demand system further

comprising:

an optional field containing optional data that may describe said demand more

precisely **(Simmons: Title and/or code can be transmitted, [0050] and [0052]),**

a Format Identifier field for defining a format of said demand short message, a

Demand Time field for indicating a time for sending said demand **('SSL': page 6**

numerals 1-3);

where said Authentication field is an encrypted digest of the above User Identifier

field, Program Identifier field, Format Identifier field, Demand Time field, Playback Time

field, and Optional field **('SSL': where the article teaches that for giving more**

security while transmitting, all data transmitted is encrypted using different level

of ciphers such as MD5, which creates a digest of the message (all fields

transmitted) (pages 2 and 3, paragraphs 11 and 12; or table 1 listing all the

ciphers that support key exchange).

On the other hand, the combined teachings of Simmons, the 'SSL' reference and Lupulescu do not explicitly teach a Playback Time field for indicating a start time of video playing.

However, in an analogous art, Needham teaches a video-on-demand system in which the user is able to select the time of download and further playback ([0020]).

Therefore, it would have been obvious to an ordinary skilled in the art at the time of the invention to have modified Simmons, the "SSL" reference and Lupulescu's invention with Needham's selection of the time of download and playback for the benefit of finding a time of the day where more bandwidth and processing power is available (Needham, [0020]).

Regarding claims 5, 13 and 20, the combined teachings of Simmons, the 'SSL' reference, Lupulescu and Needham teach a Video-on-Demand system (with respective method and computer readable medium) wherein said Authentication field is generated according to the following procedure:

Calculating the digest of all the fields except the Authentication field using a digest algorithm **("Introduction to SSL": The MD5 algorithm calculates a digest of the message (page 2 paragraph 11) excepting the Authentication field which is an encrypted result of said digest, as per claim 4)**;

encrypting with a cipher algorithm a calculated digest by adopting a secret authentication key corresponding to a user end device, uniquely allocated in advance by the program delivering end **("Introduction to SSL": Table 1 lists all the**

ciphers or algorithms that support key exchange. The process of exchanging the

keys between server and client is explained in page 6 numerals 1-10. In other

words, before sending or transmitting anything a set of keys and ciphers are

established and all messages are encrypted with them, as for example the digest

of the message); and

a process of authenticating a user's legality by the program delivering end being

conducted according to the following procedures:

calculating the digest of all the fields except the Authentication field using

a digest algorithm; encrypting with a cipher algorithm the calculated digest by adopting

a secret authentication key corresponding to a user end device, uniquely allocated in

advance by the program delivering end, so as to calculate an Authentication field; and

checking whether the calculated Authentication field and the received **(It is well known**

that the MD5 algorithm provides a way for verifying transmitted data and for

"compressing" data before being encrypted with a private key –as a matter of

example, see attached "MD5-Digest Algorithm" document. Therefore, after

decrypting the message using the keys exchanged between client and server as

described above, it is inherent that the server has to calculate a digest of the

transmitted data in order to compare it with the received digest received from the

client).

Regarding claims 6 and 14, the combined teachings of Simmons, the 'SSL'

reference, Lupulescu and Needham teach a Video-on-Demand system (with respective

method and computer readable medium), wherein when said video program is sent via

a conditional access system, a content key is delivered with the video program, so there is no need for a separate deliver of said reply message **(Simmons: [0040], [0045] and [0048])**.

Regarding claims 7, 8, 15 and 16, the combined teachings of Simmons, the 'SSL' reference, Lupulescu and Needham teach a Video-on-Demand system (with respective method and computer readable medium) wherein when the video program demanded by the user needs to be encrypted and the encrypt key is not sent via a conditional access system, the method further comprising the steps of:

generating, at the program delivering end, an encrypted reply message containing a content key of said video program, and sending it to the user end decrypting, at the user end, the content key from said encrypted reply message; and **(When establishing communication with the server, and after sending the client information for authentication, a key from the server is sent to the server to decrypt all the information sent from the server: "Introduction to SSL", page 6 numerals 6-10);**

decrypting the video program received from the program delivering end according to the decrypted content key **(Simmons, [0040], [0045] and [0052]).**

Regarding claim 21, the combined teachings of Simmons, the 'SSL' reference, Lupulescu and Needham teach a Video-on-Demand system (with respective method and computer readable medium) a short message generating means according to claim

20, wherein said digest algorithm is MD5 algorithm, and said cipher algorithm is 3DES

algorithm (**"Introduction to SSL", pages 2 and 3, paragraphs 11 and 12; or table 1**

listing all the ciphers that use support key exchange).

6.   Claims **34-37** are rejected under 35 U.S.C. 103(a) as being unpatentable over

Simmons et al. (hereinafter 'Simmons', Corrected Pub. No. 2006/0085821, of record) in

view of NPL document "Introduction to SSL" (hereinafter 'SSL' reference, of record) in

view of Lupulescu et al. (hereinafter 'Lupulescu', Pub. No. 2003/0030751) in further

view of Wiedeman et al. (hereinafter 'Wiedeman', Pub. No. 2002/0032799).

        Regarding claims 34-37, the combined teachings of Simmons, the 'SSL'

reference and Lupulescu teach all the limitations of the claims they depend on. On the

other hand, their combined teachings do not explicitly disclose wherein the sum of the

lengths of the fields does not exceed 100 bytes.

        However, Wiedeman teaches a system that sends a request message wirelessly

from a cell phone to a server on the internet through a satellite (Abstract; [0008]-[0011]).

The request messages from the cell phone are as usual small messages (i.e. 100 bytes

or less, [0035]).

        Therefore, it would have been obvious to an ordinary skilled in the art at the time

of the invention to have modified Simmons, 'SSL' reference and Lupulescu's invention

with Wiedeman's feature of sending small requesting messages (100 bytes or less) for

the benefit of 'being more efficient than having to make a DNS query first from the
device' (Wiedeman: [0035]).

Conclusion

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to OMAR PARRA whose telephone number is (571)270-
1449. The examiner can normally be reached on 9-6 PM (M-F, every other Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, John W. Miller can be reached on 571-272-7353. The fax phone number for
the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system. Status information for
published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only.
For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a
USPTO Customer Service Representative or access to the automated information
system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OP

/Hunter B. Lonsberry/

Primary Examiner, Art Unit 2421